CLAIMS

What is claimed is:

Sub B A1 ~~1. A method of determining a public key having a reduced length and a factor p,~~ using GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6), comprising the steps of:

selecting a number q and a number p such that p**2 – p + 1 is an integer multiple of q;

selecting a number g of order q, where g and its conjugates can be represented by B, where Fg(x) = x**3 - Bx**2 + (B**p)x -1 and the roots are g, g**(p-1), g**(-p);

representing the powers of g using their trace over the field GF(p^2);

selecting a private key; and

~~computing a public key as a function of g.~~

2. A method of encrypting a message using the public key generated by the method of claim 1.

3. A method of decrypting a message using the public and private key generated by the method of claim 1.

4. A method of signing a message using the public and private key generated by the method of claim 1.

5. A method of verifying a signature using the public key generated by the method of claim 1.

6. A method of Diffie Hellman key exchange and related schemes using the public key generated by the method of claim 1.

Sub A21

7. A system for ~~determining a public key~~ having a reduced length and a factor p, using GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6), comprising:

a processor for selecting a number q and a number p such that p**2 – p + 1 is an integer multiple of q;

said processor selecting a number g of order q, where g and its conjugates can be represented by B, where Fg(x) = x**3 - Bx**2 + (B**p)x -1 and the roots are g, g**(p-1), g**(-p);

said processor representing the powers of g using their trace over the field GF(p^2);

said processor selecting a private key;

a memory coupled to said processor for storing the private key;

said processor computing a public key as a function of g; and

a network interface for ~~distributing said public key~~ over a network.

8. A system of encrypting a message using the public key generated by the system of claim 7.

9. A system of decrypting a message using the public and private key generated by the system of claim 7.

10. A system of signing a message using the public and private key generated by the system of claim 7.

11. A system of verifying a signature using the public key generated by the system of claim 7.

12. A system of Diffie Hellman key exchange and related schemes using the public key generated by the system of claim 7.

Sub A3

~~13. A computer program~~ article of manufacture, comprising:

a computer readable medium for determining a public key having a reduced length and a factor p, using GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6), ~~comprising:~~

a computer program means in said computer readable medium, for selecting a number q and a number p such that p**2 – p + 1 is an integer multiple of q;

a computer program means in said computer readable medium, for selecting a number g of order q, where g and its conjugates can be represented by B, where Fg(x) = x**3 - Bx**2 + (B**p)x -1 and the roots are g, g**(p-1), g**(-p);

a computer program means in said computer readable medium, for representing the powers of g using their trace over the field GF(p^2);

a computer program means in said computer readable medium, for selecting a private key; and

a computer program means in said computer readable medium, for computing a ~~public key as a function of g.~~

14. The article of manufacture of claim 13, which further comprises:

a computer program means in said computer readable medium, for encrypting a message using the public key.

15. The article of manufacture of claim 13, which further comprises:

a computer program means in said computer readable medium, for decrypting a message using the public and private key.

16. The article of manufacture of claim 13, which further comprises:

a computer program means in said computer readable medium, for signing a message using the public and private key.

17. The article of manufacture of claim 13, which further comprises:

a computer program means in said computer readable medium, for verifying a signature using the public key.

18. The article of manufacture of claim 13, which further comprises:

a computer program means in said computer readable medium, for Diffie Hellman key exchange and related schemes using the public key.

Sub A47

~~19.~~ ~~A business method of determining~~ a public key having a reduced length and a factor ~~p,~~ using GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6), comprising the steps of:

selecting a number q and a number p such that p**2 – p + 1 is an integer multiple of q;

selecting a number g of order q, where g and its conjugates can be represented by B, where Fg(x) = x**3 - Bx**2 + (B**p)x -1 and the roots are g, g**(p-1), g**(-p);

representing the powers of g using their trace over the field GF(p^2);

selecting a private key; and

computing a ~~public key as a~~ function of g.

20. A method of encrypting a message using the public key generated by the business method of claim 19.

21. The method of decrypting a message using the public and private key generated by the business method of claim 19.

22. The method of signing a message using the public and private key generated by the business method of claim 19.

23. The method of verifying a signature using the public key generated by the business method of claim 19.

24. The method of Diffie Hellman key exchange and related schemes using the public key generated by the business method of claim 19.

B

add C1 B3